CalPSAB Approved Security Guidelines

1. Security Guideline 5.1 – Information Security (Organization & Responsibility)

(Board Approved – Dec 9, 2010)
An entity shall identify the entity's primary security official who is responsible for implementation and compliance to these guidelines. Such official shall be identified in such a way that anyone who might have a security issue or concern may contact that person.
[45 C.F.R § 164.308 (a)(2)]

2. Security Guideline 5.1.4 – Isolating Health Care Clearinghouse Functions

(Board Approved – Dec 9, 2010)
If a health care transaction clearinghouse is part of a larger entity, the clearinghouse segment shall protect and isolate individual health information of the clearinghouse from unauthorized access by the larger organization.
[45 C.F.R. § 164.308 (a)(4)(ii)(A)]

3. Security Guideline 5.2 – Risk Management Program

(Board Approved – Dec 9, 2010)
An entity shall develop and implement a risk management program that enables the entity to assess and reduce risk to an acceptable level.
[45 C.F.R. § 164.308 (a)(1)(i)]

4. Security Guideline 5.2.1 – Risk Assessment

(Board Approved – Dec 9, 2010)
An entity shall periodically conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of individual health information held, created, processed, transmitted or received by an entity.
[45 C.F.R. § 164.308 (a)(1)(ii)(A)]

5. Security Guideline 5.2.2 – Risk Management & Mitigation

(Board Approved – Dec 9, 2010)
An entity shall implement security measures sufficient to reduce risks and vulnerabilities to:

- Protect the confidentiality, integrity, and availability of all individual health information the entity creates, receives, maintains, or transmits.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under these guidelines.
- Take steps to ensure compliance with these guidelines by its workforce.

[45 C.F.R. §§ 164.308 (a)(1)(ii)(B) & 164.306 (a)]

6. Security Guideline 5.4.3 – Workforce Sanctions & Accountability

(Board Approved – Dec 9, 2010)
An entity shall apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the entity.
[45 C.F.R. § 164.308 (a)(1)(ii)(C)]

7. Security Guideline 5.4.4 – Permitted Use of Equipment

(Board Approved – Dec 9, 2010)
An entity shall specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation, including but not limited to, mobile computing devices that can access individual health information.
[45 C.F.R. § 164.310 (b)]

8. Security Guideline 5.9 – Frequency of Actions

(Board Approved – Dec 9, 2010)
Activities required by these guidelines shall be performed at a frequency determined by an entity based on knowledge of activities and/or changes within the organization, or as required by other legal or contractual obligations.
[CalPSAB Security Committee Council]

9. Security Guideline 7.1 – Facility Access Controls

(Board Approved – Dec 9, 2010)
An entity shall limit physical access to its information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
[45 C.F.R. § 164.310 (a)(1)]

10. Security Guideline 7.1.1 – Physical Access Management

(Board Approved – Dec 9, 2010)

An entity shall safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft, including procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

An entity shall document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks)
[45 C.F.R. §§§ 164.310 (a)(2)(ii) & 164.310 (a)(2)(iii) & 164.310 (a)(2)(iv)]

11. Security Guideline 7.1.2 – Communications and Operations Management

(Board Approved – Dec 9, 2010)
An entity shall assign responsibilities for the management and operation of all information processing facilities that handle individual health information.

An entity shall establish formal exchange policies, procedures, and controls to protect the exchange of information through the use of all types of communication facilities.
[ISO 10.1 Operational Procedures and Responsibilities, 10.8 Exchange of Information]

12. Security Guideline 7.3 – Technical Controls

(Board Approved – Dec 9, 2010)
An entity shall protect individual health information in information systems as specified in the guidelines.
[45 C.F.R. § 164.312(a)]

13. Security Guideline 7.3.1 – Log-In Monitoring

(Board Approved – Dec 9, 2010)
An entity shall monitor log-in attempts, reporting discrepancies, and take actions to remediate, as appropriate.
[45 C.F.R. § 164.308 (a)(5)(ii)(C)]

14. Security Guideline 7.3.3 – Malicious Code Protection

(Board Approved – Dec 9, 2010)
An entity shall take appropriate steps to protect against malicious software. In addition, an entity shall incorporate a mechanism to detect, mitigate and immediately report malicious software to the primary security official or designee for response if necessary.
[45 C.F.R. § 164.308 (a)(5)(ii)(B)]

15. Security Guideline 7.3.6 – Audit Controls

(Board Approved – Dec 9, 2010)

An entity shall implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use individual health information.
[45 C.F.R. § 164.312 (b)]

16. Security Guideline 7.4.1 – Perimeter Controls and Management

(Board Approved – Dec 9, 2010)
An entity shall identify and include, or reference, security features, service levels, and management requirements of all network services in any network services agreement, whether these services are provided in-house or outsourced. Network services include the provision of connections, private network services, and value added networks and managed network security solutions such as firewalls and a system to detect intrusion.
[ISO 10.6.2 Security of Network Services]

17. Security Guideline 7.4.3 – Intrusion Detection

(Board Approved – Dec 9, 2010)
An entity shall implement an internal system to detect intrusion attempts. The entity shall document and report successful intrusions to the primary security official or designee for response.
[NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS)]

18. Security Guideline 7.4.5 – Consistent Time

(Board Approved – Dec 9, 2010)
An entity shall take steps to ensure clocks of all relevant information processing systems within an organization are synchronized using an accurate reference time source using the Network Time Protocol (NTP).
[CalPSAB Security Committee Council]

19. Security Guideline 8.1 – Access Controls

(Board Approved – Dec 9, 2010)
An entity shall utilize identity management, authentication, and authorization mechanisms to ensure that only authorized users have access to information systems.
[45 C.F.R. § 164.312 (a)]

20. Security Guideline 8.1.2 Single Entity Authentication (Non-Federated)

(Board Approved – Sep 2009)
An entity shall authenticate each authorized user's identity prior to providing access to individual health information.

An entity shall assign a unique name and/or number for identifying and tracking user identity and implement procedures to verify that a person or entity seeking access to individual health information is the one claimed.

An entity shall authenticate each user to the level of authorized access that complies with the entity's level of trust agreement with the external exchange entity.

An entity shall authenticate users attempting to access individually identifiable health information from an unsecured location or device, shall require NIST Level 3 authentication in which the data requester must establish two factors of authentication. [*See NIST SP 800-63 Rev-1*]

[45 C.F.R. §§ 164.312 (a)(2)(i) & 164.312 (d), NIST SP 800-63 Rev 1 Electronic Authentication Guideline, OMB Safeguarding Against and Responding to the Breach of Personally Identifiable Information M 07-16]

21. Security Guideline 8.1.3 Authentication Across Multiple Entities (Federated)

(Board Approved – Sep 2009)

If an entity is participating in a trust network HIE:

- The trust network shall manage entity authentication for those participating on the trust network, and
- An entity shall manage user authentication only for those entities participating on the trust network.

If the user authentication process is across multiple systems or entities, an entity shall implement the agreed upon authentication process among the participants in the trust network.

An entity participating in the trust network shall implement a trust agreement. *[See Guideline 4.9 Contracts and Agreements]*

> *For example, an entity may use an Interconnections Security Agreement (ISA) and Memorandum of Understanding (MOU) in accordance with NIST SP 800-47 Federal Security Guide for Interconnecting Information Technology Systems, unless such requirement has been superseded by implementation of the national Data Use and Reciprocal Support Agreement (DURSA).*

The entity shall adopt an authentication solution that incorporates the authorization requirement of these guidelines. See Guideline 8.1.4 *Authorization & Access Control*.

[CalPSAB Security Access Controls Comparative Analysis]

22. Security Guideline 8.1.4 Authorization & Access Control

(Board Approved – Sep 2009)

An entity shall use the following access control attributes to determine if a user is authorized to access requested information in a way that corresponds to, and is compliant with, the data use agreements governing such access and as it aligns with state requirements:

(1) Data Source;
(2) Entity of Requestor;
(3) Role of Requestor;
(4) Use of Data;
(5) Sensitivity of Data;
(6) Consent Directives of the Data Subject

An entity that acts as a data requestor shall execute the authorization process at the location agreed upon in the data use agreements governing that exchange. The data requestor shall pass the authentication and authorization to the data supplier as a single message if so designated by the data use agreement.

[CalPSAB *Security Access Controls Comparative Analysis*

23. Security Guideline 8.2 – Data Assurance

(Board Approved – Dec 9, 2010)

An entity shall protect individual health information from unauthorized alteration or destruction.

An entity shall implement technical security measures to guard against unauthorized access to, or modification of, individual health information that is being transmitted over an electronic communications network.
[45 C.F.R. §§ 164.312 (c)(1) & 164.312 (e)(1)]